Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of authenticating communication between a first and a second party, the method comprising:

determining whether a shared secret exists between a first party and a second party;

~~provisioning a shared secret between the first party and the second party, the provisioning a shared secret comprises~~

establishing a first secure tunnel between the first party and ~~a server~~ the second party using asymmetric encryption; [[and]]

receiving the shared secret via the first secure tunnel between the first party and the ~~server~~ second party responsive to determining that a shared secret does not exist;

establishing a subsequent secure tunnel between the first party and the second party using symmetric encryption and the shared secret; [[and]]

mutually deriving a tunnel key for the subsequent secure tunnel using symmetric cryptography based on the shared secret; and

authenticating a relationship between the first party and the second party within the subsequent secure tunnel.

2. (Original) The method set forth in claim 1 further comprising the step of protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user.

3. (Currently Amended) The method set forth in claim 1 wherein the step of ~~provisioning~~ establishing a secure tunnel and receiving a shared secret occurs within a wired implementation.

4. (Currently Amended) The method set forth in claim 1 wherein the step of ~~provisioning~~ establishing a secure tunnel and receiving a shared secret occurs within a wireless implementation.

5. (Previously Presented) The method set forth in claim 1 wherein the shared secret is a protected access credential (PAC).

6. (Original) The method set forth in claim 5 wherein the protected access credential includes a protected access credential key.

7. (Original) The method set forth in claim 6 wherein the protected access credential key is a strong entropy key.

8. (Original) The method set forth in claim 7 wherein the entropy key is a 32-octet key.

9. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential opaque element.

10. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential information element.

11. (Currently Amended) The method set forth in claim 1 wherein the step of ~~provisioning~~ establishing a secure tunnel and receiving a shared secret occurs through out-of-band mechanisms.

12. (Currently Amended) The method set forth in claim 1 wherein the step of ~~provisioning~~ establishing a secure tunnel and receiving a shared secret occurs through in-band mechanisms.

13. (Cancelled)

14. (Previously Presented) The method set forth in claim 1, wherein the step of establishing a tunnel key further includes the step of establishing a session_key_seed deriving a master session key used for authenticating the relationship.

15. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using EAP-GTC.

16. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

17. (Currently Amended) A system for communicating via a network, the system comprising:

means for providing a communication link between a first party and a second party;

means for determining whether a shared secret exists between the first party and the second party;

means for provisioning a shared secret between the first and the second party responsive to the means for determining whether the shared secret exists determining the shared secret does not exist,, the means for provisioning comprises means for establishing a first secure tunnel ~~with a server~~ using asymmetric encryption and acquiring the shared secret through the first secure tunnel;

means for establishing a subsequent secure tunnel utilizing the shared secret, the means for establishing comprises means for deriving a tunnel key using symmetric cryptography based on the shared secret; and

means for authenticating a relationship between the first party and the second party within the subsequent secure tunnel.

18. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wireless network.

19. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wired network.

20. (Original) The system for communicating set forth in claim 17 wherein the shared secret is a protected access credential (PAC).

21. (Original) The system for communicating set forth in claim 18 wherein the wireless network is an 802.11 wireless network.

Claims 22 -23 (Cancelled)

24. (Currently Amended) A wireless device, comprising:

a wireless network adapter for sending and receiving signals with a second wireless device;

wherein the wireless device is configured to determine whether a shared secret exists between the wireless device and a second wireless device;

wherein the wireless ~~client~~ device is configured to receive a shared secret between the wireless ~~client~~ device and a second wireless device, upon determining that a shared secret does not exist, by establishing a first secure tunnel with a server using asymmetric encryption, wherein the shared secret is received via the first secure tunnel;

wherein the wireless ~~client~~ device is configured to establish a subsequent secure tunnel between the wireless ~~client~~ device and the second wireless device using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret; and

wherein the wireless ~~client~~ device is configured to mutually authenticate with the second wireless device employing the subsequent secure tunnel.

25. (Canceled)

26. (Previously Presented) A wireless device according to claim 24, the wireless device is configured to establish a secure tunnel further comprises establishing a session key seed for deriving a master session key used for mutually authenticating the second wireless device employing the secure tunnel.

27. (Previously Presented) A method according to claim 1, further comprising establishing a plurality of subsequent secure tunnels between the first party and second party using the shared secret acquired from the server during provisioning.